# サイバーセキュリティの社会的側面

**要　旨**

情報通信技術が急速に普及し人々の生活に浸透する反面、新たな社会的問題が多く顕在化している。パーソナルデータを含むビッグデータの政府・企業による利活用が期待される中、今後のプライバシー保護の在り方が国内外で議論されている。また、SNSの急速な普及に伴い、これらを悪用した新たなサイバー犯罪・トラブルが発生しており、子どもが巻き込まれる事例も増えている。また、主要なSNSが全世界でユーザを拡大する中で、政治的な主張を拡散する上でも強力なツールとなっており、中東や香港における民主化運動の原動力となる一方、過激派組織のプロパガンダとして利用されるなど、負の側面も見せている。

本報告書では、サイバーセキュリティを、情報通信技術を利用する環境の安全性を確保するための幅広い取組として捉えている。そこで、本論では情報通信技術の進展が社会にもたらす影響に視点を置き、現状と課題を述べる。具体的には、近年新たな問題となっている、インターネット上のプライバシー保護をめぐる課題、インターネット・SNS利用に起因する犯罪・トラブルの急増、インターネット上の経済活動の拡大、インターネットの政治への影響力の拡大についてとりあげる。

## I　インターネット上のプライバシー保護をめぐる課題

情報通信技術の急速な発展と普及に伴い、個人に関する情報（パーソナルデータ）を含む多種多様かつ膨大なデータ（ビッグデータ）がネットワークを通じて流通する社会が実現している。政府や企業によるビッグデータの活用に対する期待が高まる一方で、個人に関する大量の情報が集積・利用されることによるプライバシーの侵害に関する懸念が高まっている。実際に既存の制度によるプライバシー保護の仕組みでは、現実に起きている変化や問題に対応できない状況が発生しており、国内外で新たなプライバシー保護の仕組みの構築に向けた取組が進められている。

### 1　国内外の動向

（1）　米国

米国におけるプライバシー保護の枠組みは、連邦行政機関に対しては1974年に制定されたプライバシー法（Privacy Act of 1974, P.L. 93-579）及び2002年に制定された電子政府法（E-Government Act of 2002, P.L. 107-347）によって規制されている。民間分野に関しては、医療保険のHIPPA法（Health Insurance Portability and Accountability Act of 1996, P.L. 104-191）等、一部個別法はあるものの、多くの民間事業者には自主規制という形で裁量を与える一方、事業者が掲げるプライバシーポリシーが不適切であったり、プライバシーポリシーとは違う運用がされている場合は、連邦取引委員会法（Federal Trade Commission Act of 1914）第5条（15 U.S.C § 45）によって、厳しい制

＊本稿におけるインターネット情報の最終アクセス日は、原則として、2015年1月13日である。

裁が課されるなど、事業者の自制を促す枠組みを整備している。

2012年2月には、ホワイトハウスから、政策大綱「ネットワーク化された世界における消費者データプライバシー：プライバシーの保護とグローバルデジタル経済の革新を促進するフレームワーク」(1)が公表され、同レポートの中で情報社会における消費者プライバシー保護のフレームワークとして「消費者プライバシー権利章典」（Consumer Privacy Bill of Rights）が示された(2)。さらに2014年5月にはオバマ大統領の指示を受けたインターネット上の新たなプライバシー保護のための検討チームが、企業、研究機関、政府機関等へのヒアリング、一般向けのシンポジウムで得た意見等を基に「ビッグデータ：機会を逃さず、価値を守る」(3)と題した報告書をとりまとめ、大統領に提出した。同報告書ではビッグデータの活用に伴うプライバシー等の問題をクリアし、ビッグデータの便益を享受するため、前述の「消費者プライバシー権利章典」の法制化の検討等を含む、ビッグデータの活用を実現する法制度の構築を提言している。

### （2） OECD

経済協力開発機構（Organisation for Economic Co-operation and Development: OECD）では、現在の日本の個人情報保護法制の基礎となっている「プライバシー保護と個人データの国際流通についてのガイドライン」（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECDプライバシーガイドライン）(4)を1980年に策定しているが、同ガイドラインの策定以後30年間で、流通する個人データ(5)の量や経済的価値、プライバシー侵害のリスク、個人データの国際的利用可能性等が大きく変化したことを踏まえ、2013年にガイドラインが改正された(6)。改正ガイドラインでは、加盟国が国内でガイドラインを適用する際の8つの原則(7)に変更はなかったが、1980年のガイドラインでは明示的には要求されていないプライバシー執行機関（プライバシーを保護する法の執行に係る責任、権限を有する公的機関）の設立及び維持を加盟国に求めるほか、データ管理者である企業に対して、管理する個人データに対してリスク評価に基づく適切な保護措置等を実施することを求めた「プライバシー・マネジメント・プログラム」の構築等を求めている(8)。

---

(1)　The White House,“Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,”February 2012. <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>

(2)　同上, pp.47-48. 消費者プライバシー権利章典は、①個人のコントロール、②透明性、③コンテキストの尊重、④セキュリティ、⑤アクセスと正確性、⑥制限的収集、⑦責任の7原則からなっている。

(3)　Executive Office of the President,“Big Data: Seizing Opportunities, Preserving Values,”May 2014. <http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf>

(4)　Organisation for Economic Co-operation and Development,“OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,”September 23, 1980. <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation>

(5)　OECDプライバシーガイドラインの中で、「個人データ」は、「「個人データ」とは、識別された又は識別されうる個人（データ主体）に関するすべての情報を意味する」と定義されている。「プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告（1980年9月）（仮訳）勧告付属文書プライバシー保護と個人データの国際流通についてのガイドライン」外務省ウェブサイト <http://www.mofa.go.jp/mofaj/gaiko/oecd/privacy.html>;　同上

(6)　Organisation for Economic Co-operation and Development,“Part I. The OECD Privacy Guidelines,”*The OECD Privacy Framework*, 2013, pp.9-126. <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>

(7)　8つの原則とは、①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全保護の原則、⑥公開の原則、⑦個人参加の原則、⑧責任の原則である。

(8)　Organisation for Economic Co-operation and Development, *op.cit*. (6), p.16.

（3）　欧州

EUでは、欧州委員会が既存のEUデータ保護指令（Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data）の包括的な改正に向けて、2012年1月、EUデータ保護規則案を公表し、その後修正を経て2014年3月、欧州議会第一読会において修正案が採択されており(9)、2015年に成立が見込まれている。この改正によりEU加盟国が各国内法で対応する指令から、強制力を持ちEU加盟国へ直接適用される規則に格上げされる。また、現行のEUデータ保護指令では、企業がEU域内でデータ処理を行う場合のみ、規制の対象となっていたが、EUデータ保護規則案では、EU域外の企業であってもEU域内に在住する個人にサービスを提供する場合には規制が適用されることになる。さらに、データ削除に関する個人の権利として、いわゆる「忘れられる権利」が尊重される内容となるなど、規制強化の面が強く、EU域内で活動する企業、またEUにサービスを提供する日本企業にも多大な対応が求められることが予想されている(10)。

（4）　日本

日本では、高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）での議論を経て、2013年6月に「世界最先端 IT 国家創造宣言」が新たなIT戦略として閣議決定された。

この中では、「「ビッグデータ」のうち、特に利用価値が高いと期待されている、個人の行動・状態等に関するデータである「パーソナルデータ」の取扱いについては、その利活用を円滑に進めるため、個人情報及びプライバシーの保護との両立を可能とする事業環境整備を進める」(11)との方針が示された。これを受けて、具体的なルールを検討する場として、2013年9月にIT総合戦略本部の下に「パーソナルデータに関する検討会」が設置され、個人情報保護法改正に向けた検討を行った。同検討会の活動成果として、2014年6月24日、「パーソナルデータの利活用に関する制度改正大綱」(12)がIT総合戦略本部によって決定された。同年7月に実施されたパブリックコメントを踏まえて、関係法案の作成に着手し、2015年1月以降、可能な限り早期に国会に法案を提出するとしている。また、個人情報の取扱いに関しては、諸外国ではすでに独立的な立場から監視・監督を行う第三者機関（プライバシーコミッショナー）が導入されている。国内でも早期の設立が求められていた(13)が、同大綱においては、「行政手続における特定の個

(9)　European Parliament, "European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)　(COM(2012) 0011 – C7-0025/2012 – 2012/0011 (COD))," March 2014. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN>

(10)　当初の規則案では、既存のデータ保護指令にあった「データ消去権等」に加え、より明確な権利として「忘れられる権利（right to be forgotten）」を規定していた。修正案では「忘れられる権利」の文言は削られ、単に「消去権」とされたものの、「消去権」が「忘れられる権利」を包含するとされている。

(11)　「世界最先端 IT 国家創造宣言について」（平成25年6月14日閣議決定）p.7. <http://www.kantei.go.jp/jp/singi/it2/pdf/it_kokkasouzousengen.pdf>

(12)　高度情報通信ネットワーク社会推進戦略本部「パーソナルデータの利活用に関する制度改正大綱」2014.6.24. <http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf>

(13)　総務省「パーソナルデータの利用・流通に関する研究会報告書―パーソナルデータの適正な利用・流通の促進に向けた方策―」2013.6, pp.36-37. <http://www.soumu.go.jp/main_content/000231357.pdf>; 日本弁護士連合会「日本版プライバシー・コミッショナーの早期創設を求める意見書」2014.2.21. <http://www.nichibenren.or.jp/library/ja/opinion/report/data/2014/opinion_140221.pdf>

人を識別するための番号の利用等に関する法律」（いわゆる「番号法」。平成25年法律第27号）に規定されている特定個人情報保護委員会を改組して新たな委員会を設置し、法定事項や民間の自主規制の実効性のある運用、国際的な整合性確保等を担う第三者機関とする方針が明らかにされた(14)。なお、「世界最先端IT国家創造宣言」は2014年6月に改定されている。

## 2　最新の事例・課題

### (1)　ビッグデータの利活用

ビッグデータの活用領域は、健康・医療、防災、交通、エネルギー、農業など多岐にわたる。2013年に日本政策投資銀行が実施した調査では、5割超の企業がビッグデータを活用、活用を検討中、あるいは、活用検討の可能性があると回答しており、産業界のビッグデータの活用に対する関心の高さがうかがわれる(15)。

こうした中、企業のデータ利活用が許容されるのか不明確な「グレーゾーン」にかかわる問題が顕在化している。

2013年6月、東日本旅客鉄道（JR東日本）が、同社が提供する交通・ショッピングに使用可能なICカードSuicaの利用データから氏名、電話番号、物販情報を除外したり、Suica番号を不可逆の別異の番号に変換したりする等の匿名化処理を施したデータを、日立製作所に提供（提供は同年7月に実施予定）することが明らかになり、同社に対して多くの利用者やメディアから個人情報の保護、プライバシーの保護、消費者意識に対する配慮がかけているのではないかとして批判や懸念が寄せられた。JR東日本ではホームページへのFAQ（Frequently Asked Questions）の掲載やデータ提供除外（オプトアウト）に関する案内等で利用者に説明を行うとともに、2013年9月には社外の専門家からなる有識者会議を設置し、①Suicaに関するデータの社外への提供に関する問題の整理、②今後の社外への提供について検討を行った。同有識者会議の中間とりまとめにおいては、①に関しては、「事前に十分な説明や周知を行わなかったことなど、利用者への配慮が不足していたことは問題であり、JR東日本という公共性の高い企業の立場からも、利用者に不安を与えた事実を重く受け止める必要がある」と指摘した。一方で、プライバシーの保護に関しては、「一定レベルの匿名化処理や日立製作所との間で特定の個人を識別することを禁止する契約を締結しているので、直ちに個人のプライバシーが侵害されるおそれはないと判断される」とした。(16)

今後のSuicaに関するデータの社外への提供については、有識者会議において「法改正の動向等を注視しながら検討する必要がある」とのアドバイスを受けたことから、JR東日本では引き続きデータ提供を見合わせる判断を行った(17)。こうした事例が問題になったことで事業者が社会的批判を懸念して、問題のないビッグデータの利活用に躊躇する（いわゆる「利活用の壁」）事例も出ており、保護すべき情報の範囲や事業者が遵守すべきルールについて現行法の

(14)　高度情報通信ネットワーク社会推進戦略本部　前掲注(12), pp.13-15.
(15)　日本政策投資銀行「第3編　企業行動に関する意識調査」『調査』106号, 2013.9, p.87. <http://www.dbj.jp/investigate/r_report/pdf_all/106all_3.pdf>
(16)　東日本旅客鉄道「Suicaに関するデータの社外への提供についての有識者会議「中間とりまとめ」の概要」2014.3.20, p.2. <http://www.jreast.co.jp/chukantorimatome/gaiyo/20140320.pdf>
(17)　東日本旅客鉄道「Suica に関するデータの社外への提供についての有識者会議「中間とりまとめ」受領について」2014.3.20. <http://www.jreast.co.jp/press/2013/20140311.pdf>

曖昧な点を解消していくことが急務となっている[18]。

(2)「忘れられる権利」

また、欧州のデータ保護の新たな枠組みとなるEUデータ保護規則に実質的に盛り込まれる見込みの「忘れられる権利」に関連して、検索サイトの個人に関する検索結果の削除要求に対する国内外の司法判断が注目を集めている。欧州では、スペイン人男性がGoogle Spain及びGoogleに対して、Googleの検索結果で表示される男性に関する過去の新聞記事へのリンクを削除するように求めた裁判で、2014年に欧州司法裁判所はプライバシー保護の観点から、Google等の検索サービス事業者は一定の条件下でリンクを削除する義務があるとする裁定を下した[19]。この司法判断を受けてGoogleやMicrosoftでは欧州在住のユーザに対して検索結果のリンク削除を申し込むフォームの公開を開始している。

こうした欧米における「忘れられる権利」に関する議論の高まりを受けて、日本国内でも議論が広がっている。2014年には、検索結果の削除をめぐる事例について相次いで司法判断がなされており[20]、今後の事業者側の動向が注目されている。2014年11月には検索サイト大手のヤフーが、外部の専門家からなる「検索結果とプライバシーに関する有識者会議」を設置し、「表現の自由」や「知る権利」、プライバシーのバランスに配慮した、検索結果の削除に関する判断の在り方について検討するとしている[21]。今後は、国としてプライバシーや個人情報の保護の枠組みの中に、個人情報の削除に関する日本独自の基準を検討していく場が必要となる。

## II　インターネット・SNS利用に起因する犯罪・トラブルの急増

### 1　国内外の動向

スマートフォンやソーシャルネットワーキングサービス（Social Networking Service: SNS）の普及によって、誰とでも気軽にインターネット上でつながることができる一方で、これらに起因する様々な問題が発生している。

2013年通信利用動向調査によれば、2013年末時点のスマートフォンによる個人のインターネット利用率は全体で42.4%、年代別では6歳～12歳で18.3%、13歳～19歳で64.1%、20歳～29歳では83.3%に達する。また、個人のソーシャルメディア[22]の利用率は全体で42.4%、年代別では6歳～12歳で15.9%、13歳～19歳で57.2%、20歳～29歳で65.5%と、10代後半及び20代で5割を超えており、中高生にもスマートフォンやソーシャルメディアが広く普及している状況がうかがえる[23]。一方でこれらの利用をコントロールできず生活に支障をきたす、ネット依存、ス

(18)　高度情報通信ネットワーク社会推進戦略本部　前掲注(12), pp.6-7.
(19)　Court of Justice of the European Union, "Judgment of the Court (Grand Chamber)," May 13, 2014. <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=363285>
(20)「時流・底流：忘れられる権利　日本とEU、司法判断に差」『毎日新聞』2014.9.8;「グーグル検索結果の削除命令　記事タイトル・要約も対象 東京地裁、人格権に配慮」『日本経済新聞』2014.10.20.
(21)「検索結果とプライバシーに関する有識者会議」2014.11.7. ヤフーウェブサイト <http://publicpolicy.yahoo.co.jp/2014/11/0717.html>
(22)　インターネット上で利用者同士、相互のやり取りができる双方向のメディアであり、SNSもその1つ。
(23)「平成25年通信利用動向調査の結果（概要）」総務省ウェブサイト <http://www.soumu.go.jp/johotsusintokei/statistics/statistics05a/h25doukou.html>

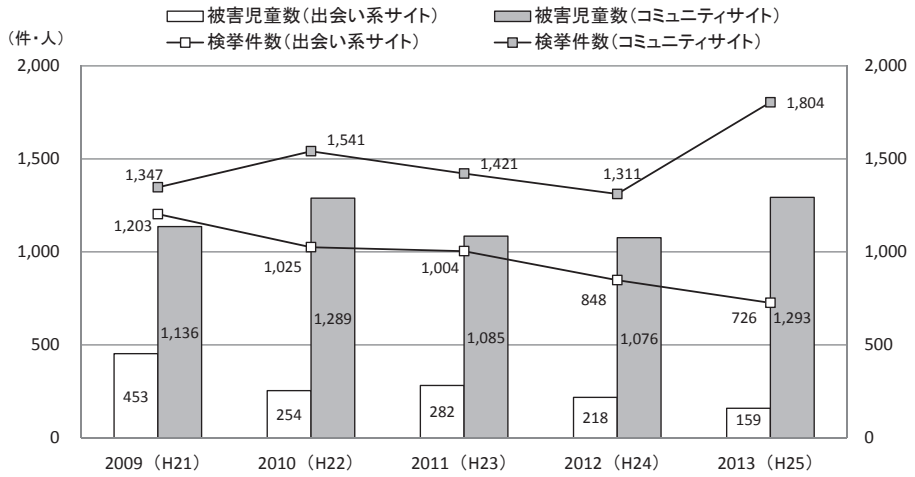
マホ依存、SNS依存といった状態に陥ってしまうケースも問題となっている。

このようにスマートフォンやSNSが幅広い世代に普及する一方、サイバー犯罪やネットいじめ、炎上、なりすまし等、様々な犯罪・トラブルに巻き込まれる事例が増加しており、子どもが被害側や加害側になるケースも多く見られる。

警察庁が発表している出会い系サイト及びコミュニティサイト(24)に起因する事犯に関するデータ（図1参照）によれば、2013（平成25）年中にコミュニティサイトに起因して犯罪被害に遭った児童は1,293人で前年比20.2%も増加している。そのうち罪種別での被害児童数は、青少年保護育成条例違反が678人と最も多く、児童買春が226人となっている。

コミュニケーションツールの変化にともない、犯罪が発生する場や手口も変化している。警察庁の調査では、かつて児童の犯罪被害の温床となっていた出会い系サイトに起因して犯罪被害に遭った児童は159人で前年比27.1%減と、2008年に「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」（いわゆる「出会い系サイト規制法」。平成15年法律第83号）を改正する「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律の一部を改正する法律」（平成20年法律第52号）が施行されて以降、禁止誘引違反者の検挙や無届けサイトの取締り等により減少傾向にあるが(25)、実際にはコミュニティサイトが出会い系サイトと同じ目的で使われており、問題の根本的解決には至っていないのが実態である。

図1　出会い系サイト及びコミュニティサイトに起因する被害児童数の対比




（出典）警察庁「平成25年中の出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について」2014.2.27, p.2. <https://www.npa.go.jp/cyber/statics/h25/pdf02-2.pdf>を基に三菱総合研究所作成。

## 2　代表的な事例と対策状況

インターネット・SNS利用に起因する犯罪・トラブルに関する最近の代表的な事例として、

(24) SNS等、共通の自己のプロフィール等を掲載し、仲間を増やしていくようなサイト。警察庁「平成23年度総合セキュリティ対策会議 第5回 発言要旨」2011.12.20, p.1. <https://www.npa.go.jp/cyber/csmeeting/h23/pdf/h23youshi5.pdf>

(25) 警察庁「平成25年中の出会い系サイト及びコミュニティサイトに起因する事犯の現状と対策について」2014.2.27, pp.1-2. <https://www.npa.go.jp/cyber/statics/h25/pdf02-2.pdf>

ID交換掲示板、ネットいじめ、リベンジポルノ、アカウント乗っ取りについて取り上げる。

（1）　ID交換掲示板

警察庁の発表によれば、近年、無料通話アプリ（LINE等）のIDを交換する掲示板（ID交換掲示板）に起因する犯罪被害が増えている。ID交換掲示板は無料通話アプリのIDを公開する掲示板であり、インターネット上に多数存在している。面識のない相手と接触するために、IDとともに「友達募集」などの短文や、居住地域、年齢、性別等の情報を公開されているうえ、それらの情報でユーザを検索できるものもあり、犯罪者に悪用されるリスクが高い。(26)

ID交換掲示板に関しては、実際には出会い系サイトと同様の目的で使われているケースが多い。しかし、現行の出会い系サイト規制法の規制の対象となる出会い系サイト（インターネット異性紹介事業）は4つの要件(27) 全てに該当するものとされ、この定義に該当しないことでID交換サイトが出会い系サイト規制法の対象とならないケースがある。こうした状況を踏まえ無料通話アプリの事業者側では異性との出会いを目的とした行為を確認した場合にはサービスの利用を停止する措置をとったり、18歳以下のユーザに対してID検索に制限を設ける等対策を講じているが、親族名義のアカウントを使ったり、ID以外の情報で連絡をとる等、対策をすり抜ける事例も多く根本的な解決には至っていない。

（2）ネットいじめ

文部科学省の調査によると2013年度の小・中・高・特別支援学校における、いじめの認知件数は185,860件（児童生徒1,000人当たりの認知件数は13.4件）である。そのうちパソコンや携帯電話等を使ったいじめは8,787件（いじめ認知件数の4.7%）であり、前年の7,855件から増加している(28)。以前は、特定の学校に関する情報を交換するための学校裏サイトがネットいじめの温床になることが多かったが、最近はLINE等のSNS上のいじめが問題視されており、表1に示すように、2013年にはLINE等のSNS上のトラブルに起因した（関連が疑われる）暴行、殺人事件や、自殺等の深刻なケースが相次いで明るみに出ている。また、海外でもFacebook上のいじめを苦にした未成年の自殺が相次いでおり、SNS等を通じたネットいじめ（Cyberbullying）は国際的な問題となっている。

(26)　同上 p.1; モバイルコンテンツ審査・運用監視機構「青少年被害が急増しているID交換掲示板に関して対応すべき青少年保護施策について」2014.5.30, pp.1, 4. <http://www.ema.or.jp/press/2014/0530_04.pdf>

(27)「インターネット異性紹介事業」は、①面識のない異性との交際を希望する者（異性交際希望者）の求めに応じて、その者の異性交際に関する情報をインターネット上の電子掲示板に掲載するサービスを提供していること、②異性交際希望者の異性交際に関する情報を公衆が閲覧できるサービスであること、③インターネット上の電子掲示板に掲載された情報を閲覧した異性交際希望者が、その情報を掲載した異性交際希望者と電子メール等を利用して相互に連絡することができるようにするサービスであること、④ 有償、無償を問わず、これらのサービスを反復継続して提供していること、の4つの要件を満たすものと定義されている。警察庁「「インターネット異性紹介事業」の定義に関するガイドライン」2008.8.7. <http://www.npa.go.jp/cyber/deai/business/images/01.pdf>

(28)　文部科学省初等中等教育局児童生徒課「平成25年度「児童生徒の問題行動等生徒指導上の諸問題に関する調査」について」2014.10.16, pp.2-3. <http://www.mext.go.jp/b_menu/houdou/26/10/__icsFiles/afieldfile/2014/10/16/1351936_01_1.pdf>

表1　ネットいじめに関連する事件

| 時期 | 事件の概要 |
|---|---|
| 2013年7月 | 広島県呉市で高等専修学校の元女子生徒（当時16歳）が少年ら6人と共謀して、元同級生の女子生徒（当時16歳）を暴行のうえ殺害、遺棄した。犯行の動機は、被害者の元女子生徒がLINEの悪口に言い返してきたことに立腹したこととされている。2014年10月24日、広島地裁は被告の元女子生徒に対して強盗殺人などの罪で、懲役13年（求刑懲役15年）の判決を言い渡した。(*1) |
| 2013年8月 | 熊本県熊本市内の県立高校の女子生徒（当時1年生）が自宅で首を吊って自殺。熊本県教育委員会は、女子生徒と同じ寮に暮らす同級生からLINE上に女子生徒の身体的特徴を揶揄する表現や、身体へ危害を加えると脅すような書込みなど4件のいじめがあったと説明した。(*2) |
| 2013年6月 | 福岡県北九州市と芦屋町に住む少女計4人が、芦屋町の高校1年の女子生徒方に侵入し、暴行を加え、顔面打撲などのけがを負わせた。4人の少女のうち別の高校の3年生と2年生の少女が被害少女と同じ中学校の出身で、被害少女がLINEで「（2年少女が）面倒くさい」などのメッセージを送ったことへの仕返しだったとしている。(*3) |
| 2014年7月 | 熊本県熊本市内の市立中学校3年生の男子生徒が薬を飲んで自殺を図り、救急搬送されて一時入院。学校が設置した調査委員会は、男子生徒が、同級生とのトラブルの中でLINEを通じて「ざまーみろ」と言われたことなど3件についていじめを受けていたことを認定したが、いじめと自殺の因果関係は「分からない」としている。(*4) |
| 2014年7月 | 青森県八戸市の県立高校2年の女子生徒が学校の昼休み中に行方不明になり、その後八戸沖で遺体が見つかった。青森県教育委員会によると、女子生徒の遺書は無かったが、いじめを示唆するメモを残しており、両親は「LINEなどをめぐりトラブルがあった」と話しているとしている。(*5) |

（＊1）「広島女子生徒殺害、元同級生に懲役13年、地裁判決」『日本経済新聞』2014.10.25.
（＊2）「県「フォローしていれば」 熊本市・高1自殺　高校、情報共有せず「解決」と認識、悲劇再び」『西日本新聞』2014.10.23.
（＊3）「少女4人傷害容疑で逮捕 「LINE」のメッセージに仕返し」『読売新聞』（北九州版）2013.10.22.
（＊4）「熊本市で中3自殺未遂　市教委、いじめ3件認定　因果関係「不明」」『読売新聞』（熊本版）2014.10.31.
（＊5）「青森の女子高生、いじめで自殺か」『日本経済新聞』2014.7.23, 夕刊.
（出典）三菱総合研究所作成。

### (3)　リベンジポルノ

リベンジポルノとは、本人の同意を得ずに、元交際者や元配偶者等の裸や性的な画像又は動画を嫌がらせの目的でインターネット上に流布する行為を指し、2013年に発生した三鷹ストーカー殺人事件で、容疑者によって被害者の画像がインターネット上に拡散されたことを受けて、国内でも広く認知されるようになった。SNSや電子メール等で執拗に嫌がらせを行うサイバーストーカー行為の一種として行われる事例も増えている。一度インターネット上に流出した画像等の情報を完全に削除することは困難であるため、被害者が受ける損害は重大であり、国内外で対応が急がれている。

現行法ではリベンジポルノは、名誉毀損、わいせつ等の罪に該当しうるほか、ストーカー行為としてリベンジポルノが行われた場合は「ストーカー行為等の規制等に関する法律」（いわゆる「ストーカー規制法」。平成12年法律第81号）の規制対象となりうる。リベンジポルノという行為自体を端的に違法行為の類型とするかは、国内で検討が続いていた。(29)

同様の問題に対して、リベンジポルノが以前から社会問題化していた米国では2003年に

(29)　ストーカー行為等の規制等の在り方に関する有識者検討会「ストーカー行為等の規制等の在り方に関する報告書」2014.8.5, p.4 <https://www.npa.go.jp/safetylife/seianki/stalker/report/report.pdf>

ニュージャージー州でリベンジポルノを違法とする州刑法改正が行われているほか、2013年から2014年にかけてリベンジポルノ罪を新設する法案が全米の多くの州議会に提出されている[30]。

こうした中、自由民主党は2014年2月にリベンジポルノ規制の新法制定に向け特命委員会を設置した。同委員会の検討を踏まえ、2014年の第187回国会（臨時会）に議員立法での法案を提出し、両院で可決・成立した。同年11月に施行されたこの「私事性的画像記録の提供等による被害の防止に関する法律」（いわゆる「リベンジポルノ防止法」。平成26年法律第126号）は画像を不特定多数に拡散させた場合、3年以下の懲役又は50万円以下の罰金を科すほか、現行の「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（いわゆる「プロバイダ責任制限法」。平成13年法律第137号）には画像の発信者に削除への同意を照会し、7日経っても反論が無ければ削除できるとする規定があるが、この期間を特例で2日に短縮するとしている[31]。

### (4)　アカウント乗っ取り

第三者にSNSのアカウントが不正にログインされ、アカウント内の情報を窃取される、勝手に投稿される、メッセージを送信されるなどのアカウント乗っ取りが多く発生している。表2に示すように、2013年頃からFacebookのアカウント乗っ取りが多く報告されたほか、2014年にはLINEのアカウントが乗っ取られる事例が多く発生し、同年6月にはLINEがアプリ内で注意喚起を行っている。第三者にアカウント情報が乗っ取られてしまう原因として、複数のインターネットサービスで同じIDとパスワードを使っている場合、ほかのサービスから流出したパスワードを使って不正にログインされることが多い。また、Facebookで友達を装った偽アカウントを使って、「信頼できる連絡先」[32]へ設定するよう誘導し、アカウントのパスワードをリセットしてしまう手口[33]やTwitterの「アプリ連携」を悪用する手口なども見られる。基本的な対策としては、推測されやすいパスワードの使用やパスワードの流用を避けることが最も重要であるが、各SNSで提供されている機能や設定を正しく理解し、適切に利用することも重要な対策となる。

(30) 井樋三枝子「アメリカにおける性的図画の流布を処罰する州法―リベンジポルノ等の犯罪化に関する各州立法動向―」『外国の立法』No.260, 2014.6, p.16. <http://dl.ndl.go.jp/view/download/digidepo_8677795_po_02600003.pdf?contentNo=1>
(31)「リベンジポルノ懲役3年、自民、法案提出へ」『日本経済新聞』2014.10.13.
(32) Facebookアカウントにアクセスできなくなった場合に、連絡が取れる友達のこと。
(33) 情報処理推進機構「「SNSの友達申請に注意！」―Facebookで乗っ取り被害に遭わないために―」2013.11.1. <https://www.ipa.go.jp/security/txt/2013/11outline.html>

表2　SNS乗っ取り被害の例

| SNS | アカウント乗っ取り被害の例 | 乗っ取りの手口の例 |
|---|---|---|
| Facebook | 2013年頃から多く発生。①情報を窃取される（アカウントのプロフィールにある個人情報や、友達に関する情報）、②勝手に「いいね！」をクリックされて、悪意のあるサイトの宣伝や誘導に加担させられる、③友達のウォール（投稿や写真を友達と共有する場所）に勝手に投稿されて、悪意あるサイトの宣伝や誘導に加担させられる、④Facebookのメッセージ機能を使ってスパムメッセージを勝手に発信させられる等の被害が発生。 | 偽アカウントで友達を装って、「信頼できる連絡先」の設定へ誘導し、その権限を使ってパスワードリセットを行い、新しいパスワードを設定する。 |
| LINE | 2014年に増加（LINEの発表では2014年6月時点でアカウント情報の外部流出によると思われる不正アクセス303件を確認。）。①LINEの友達に勝手にトークを送られる（友達のふりをして「プリペイドカード、ウェブマネーを買うのを手伝ってほしい」等と振り込め詐欺のような行為を行う。）、②勝手に有料スタンプなどを購入する、③自分のLINEアカウントが削除される等の被害が発生。 | 複数のインターネットサービスで同じパスワードを使っている場合に、ほかのサービスから流出したと思われるメールアドレスやパスワードを第三者が流用。 |
| Twitter | 2013年から多く発生。著名人や大手メディアのアカウントも多く被害に遭った。①勝手にツイートがされている、②自分のアカウントからダイレクトメッセージ（DM）が送られている、勝手に他のアカウントに対する操作がされる（フォロー、リツイート、フォロー解除、ブロック等）等の被害が発生。 | ①スパムアカウント（＊）から送られてきたツイートで「アプリ連携承認画面」へと誘導を行い、承認を行わせることで、外部アプリから勝手にツイートやフォローを行う。②TwitterやTwitterと連携するサービスを装ったサイトに誘導しパスワードを盗みだす。 |

（＊）個人情報の取得等を行う有害なページへのリンクを含む投稿を行ったり、不特定多数のユーザをフォローしたり、リツイートする等の行為を行うアカウント。
（出典）情報処理推進機構「SNSの友達申請に注意！ Facebookで乗っ取り被害に遭わないために」2013.11.1. <https://www.ipa.go.jp/security/txt/2013/11outline.html> 等を基に三菱総合研究所作成。

個別の事例に対して対策が講じられる一方、日々新たに発生する犯罪手口やトラブル事例に対応した技術的対策、法制度などを網羅的に整備することは難しく、情報通信技術を利用する個人がサイバーセキュリティに関する高いリテラシーを持ち、個人がリスクを理解した上で責任を持って使用することも重要である。

## Ⅲ　インターネット上の経済活動の拡大

### 1　インターネット上の経済活動の概況

ネットショッピング・ネットオークションや電子マネーの普及、インターネットバンキングや様々な金融商品のオンライン取引の普及に伴い、インターネット上の経済活動の規模は年々拡大している。

日本国内の2013年の消費者向け電子商取引（Electric Commerce: EC）市場規模は、約11.2兆円（前年比17.4%増）となり、電子商取引の浸透度合いを示す指標であるEC化率(34)も3.7%となって、前年から0.6ポイント上昇している。(35)

家計消費に占めるネットショッピングの割合も年々増加している。総務省の家計消費状況調

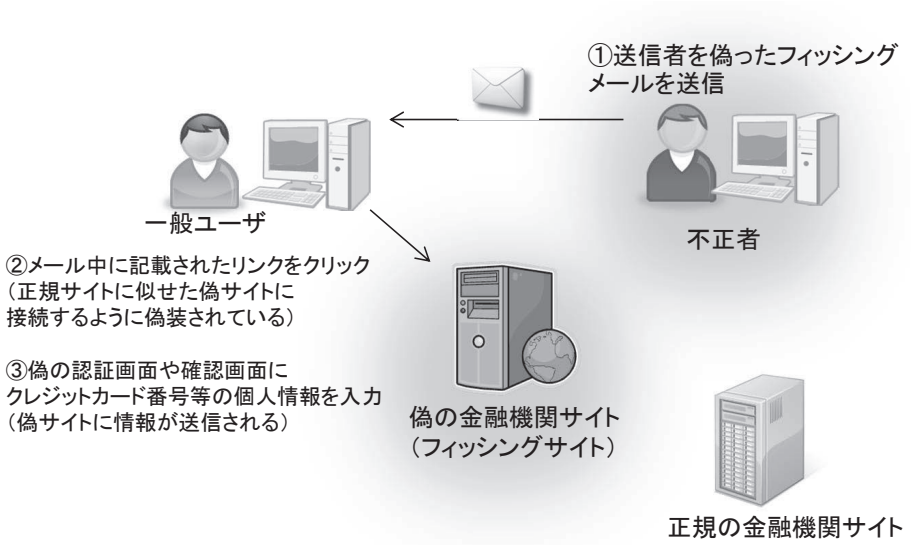
(34) 全ての商取引における、ECによる取引の割合。消費者向け電子商取引（BtoC-EC）におけるEC化率は、小売業・サービス業における値を指す。

査の2013年の調査結果によれば、二人以上の世帯のうちインターネットを利用した支出のあった世帯の割合は全体の24.3%（前年比2.7%増）となり、インターネットを利用しない世帯も含めた一世帯当たり1か月間のインターネットを利用した支出総額は5,801円（前年比14.3%増）であった(36)。

手軽にネットショッピングやネットオークションを利用できるようになった一方でトラブルも増加している。国民生活センターや全国の消費生活センターにはインターネット通販やインターネットオークションに関するトラブル事例が多く寄せられており、信頼できる業者の選定に関して注意喚起を行っている。

また、ショッピングや各種料金の支払いでもオンライン決済やインターネットバンキングの利用が普及しており、これを悪用して実在の銀行やクレジットカード、ショッピングサイトなどを装った電子メールを送付し、これらのウェブサイトに似せた偽サイトに誘導し、暗証番号などの認証情報を入力させて搾取する「フィッシング」（図2参照）の被害が急増している。フィッシングに関する情報収集や注意喚起を行うフィッシング対策協議会に対して届けられたフィッシングの件数は、2012年度が828件であったのに対し、2013年度は15,171件と17倍以上に増加している(37)。

図2　フィッシングの手口




（＊）図は正規の金融機関を装ったメール（フィッシングメール）をユーザに送り、正規の金融機関のサイトに似せた偽サイトに誘導し、そこでクレジットカード番号等の個人情報を入力させる事例。
（出典）「消費者の皆様へ」フィッシング対策協議会ウェブサイト <https://www.antiphishing.jp/consumer/abt_phishing.html>を基に三菱総合研究所作成。

(35) 経済産業省商務情報政策局情報経済課「平成25年度我が国経済社会の情報化・サービス化に係る基盤整備（電子商取引に関する市場調査）報告書」2014.8, p.6. <http://www.meti.go.jp/press/2014/08/20140826001/20140826001-4.pdf>
(36) 総務省統計局「家計消費状況調査年報（平成25年）」2014.7, pp.11-12. <http://www.stat.go.jp/data/joukyou/2013ar/gaikyou/pdf/gkall.pdf>
(37) フィッシング対策協議会ガイドライン策定ワーキンググループ「フィッシングレポート2014―急増する不正送金とフィッシング―」2014.7, pp.1-2. <https://www.antiphishing.jp/report/pdf/phishing_report_2014.pdf>

## 2　インターネット上の経済活動にかかわる犯罪・トラブルの代表的な事例と対策状況

インターネット上の経済活動にかかわる具体的な犯罪・トラブルに関する代表的な事例として、インターネット通販・インターネットオークション、不正送金、闇サイトにおける違法取引について取り上げる。

### (1)　インターネット通販・インターネットオークション

国民生活センターに寄せられる相談の中ではインターネット通販の前払いによるトラブル（前払いをしたにもかかわらず商品が届かない、注文したものと違うものが届いた等）の相談が多く、特に2013年以降急増している。ネットショッピングの場合、店舗の実態がないため、目当ての商品や安さだけで判断して、悪質な業者のサイトを利用してしまうリスクがある。インターネットオークションに関しても同様に、落札し代金を支払ったのに商品が届かない、相手と連絡が取れないという事例も多い。また、2009年から2011年にかけて入札行為自体に手数料が係る、いわゆる「ペニーオークション」(38)に関するトラブルが急増した(39)。2012年には、事実上商品が落札できない仕組みにもかかわらず「激安価格で落札できる」などと表示して顧客から入札に必要な仮想通貨を購入させた詐欺容疑で、ペニーオークションの事業者が摘発されたこともあり(40)、現在ではペニーオークションサイトは見られなくなっている。

なお、ペニーオークションに関しては、芸能人などが業者から報酬を受けとって、実際には落札していない商品をブログの中で、「激安で落札した」などと紹介したことが発覚し、大きな問題となった。この事件をきっかけに、消費者に気づかせないように宣伝・広報活動を行う「ステルスマーケティング（ステマ）」が広く注目されることになった。最近は企業のマーケティング活動の一環として、強い影響力を持つブログ運営者（芸能人や多数の読者を持つブロガー）に集中的にプロモーションを行い、ネット上で話題にしてもらうステマ手法が一般化している。また同様に影響力を持つのが、「口コミ」と呼ばれる、商品やサービス、企業に対する個人の評価である。日本ではステルスマーケティングそのものは禁止されていないが、事業者による口コミの操作などは問題事例とされている(41)。一部の行き過ぎたマーケティング活動については事業者側のモラルが問われており、2009年には健全な口コミ（Word of Mouth: WOM）マーケティングを目指す業界団体としてWOMマーケティング協議会が設立され、口コミマーケティングに関するガイドラインを公開する等の活動を行っている(42)。

(38)　一般のインターネットオークションであれば、入札には費用がかからず落札者だけが商品代金を支払うが、ペニーオークションの場合は、落札しなくとも入札するたびに手数料を支払わねばならない。さらに、入札単位が1円など少額で固定的に設定されており、入札者が自由に価格を決められないうえ、誰かが入札するたびにオークション時間が延長される仕組みのため、入札者自身がオークション終了時間を予測できず、手数料が積みあがってしまう。

(39)　国民生活センター「入札のたびに手数料が･･･！“ペニーオークション”のトラブルが急増」2011.1.24, pp.1-2. <http://www.kokusen.go.jp/pdf/n-20110124_1.pdf>

(40)「ペニーオークション：初摘発　詐欺容疑で4人逮捕　京都、大阪府警」『毎日新聞』2012.12.8.

(41)　消費者庁「「インターネット消費者取引に係る広告表示に関する景品表示法上の問題点及び留意事項」の一部改定について」2012.5.9. <http://www.caa.go.jp/representation/pdf/120509premiums_1.pdf>

(42)　WOMマーケティング協議会ウェブサイト <http://womj.jp/news/index.html>

（2）　不正送金

警察庁の発表によれば、近年インターネットバンキングに係る不正送金事犯が急増しており、2012年には64件、4800万円であった被害額が、2013年には1,315件、約14億600万円と1年間で約29倍まで膨らんでいる(43)。さらに2014年は上半期だけですでに1,254件、約18億5200万円の被害が発生している(44)。インターネットバンキングの利用者のアカウント窃取の攻撃手法として、これまではキーロガー（キーボードへの入力を記録するソフトウェア）で認証情報を盗み取ったり、銀行等サイトに似せた偽サイトに誘導するフィッシングサイトで認証情報を騙し取る、認証時の画面の画像データを盗み取るなどの攻撃が知られていたが、近年は中間者攻撃（Man-in-the-Middle攻撃）(45)と似たMITB攻撃（Man-in-the-Browser攻撃）と呼ばれる攻撃の被害が多く報告されている。MITB攻撃とは、マルウェアに感染したパソコンから正規のインターネットバンキングの正規サイトにアクセスすると、マルウェアがその通信を検知しウェブブラウザに表示される内容の一部を改ざんするなどし、本来の正規サイトでは表示されない偽の認証情報の入力フォームが表示され、そこにユーザが認証情報を入力してしまうと、利用者に気づかれない形でサイバー犯罪者の口座に自動で送金処理がされてしまう攻撃である(46)。ユーザのログイン情報を盗みとるだけの攻撃では、ワンタイムパスワード（本人認証を行うためのパスワードを毎回変更する方式）などを使って被害を防ぐことができる可能性があるが、MITB攻撃の場合はリアルタイムで送金処理が行われてしまうため被害を防ぐことが難しい。

このほかにも金銭被害の可能性がある攻撃として、マルウェアに感染したコンピュータ内のデータを暗号化するなどして、暗号化を解除する見返りとして金銭を要求するランサムウェア（身代金要求ウイルス）等の相談件数も増えている(47)。

こうした状況に対し、金融庁、金融機関、警察が中心となり注意喚起を行ったり、金融機関が専用のウイルス対策ソフトやフィッシング対策ソフトを無償配布したり、認証の強化策を導入したりしているが、前述のとおり攻撃手法が巧妙化しており、依然として被害は収まっていない。

（3）　闇サイトにおける違法取引

インターネット上の経済活動は表の市場だけでなく、違法な品物や不正に取得された情報の取引や、違法行為の請負などを行うアンダーグラウンドなサイト、いわゆる闇サイト(48)における市場（地下市場）も拡大している。サイバー犯罪にかかわる取引が行われる闇サイトも多く

(43) 警察庁「平成25年中のインターネットバンキングに係る不正送金事犯の発生状況等について」2014.1.30, pp.1-2. <https://www.npa.go.jp/cyber/pdf/H260131_banking.pdf>

(44) 警察庁「平成26年上半期のインターネットバンキングに係る不正送金事犯の発生状況について」2014.9.4, <https://www.npa.go.jp/cyber/pdf/H260904_banking.pdf>

(45) 通信を行っている当事者間に悪意を持った第三者が割り込み、不正を行う攻撃。

(46)「ネットバンキング利用者を狙う攻撃に注意喚起」2012.10.29. トレンドマイクロウェブサイト <http://www.is702.jp/news/1234/>;「2014年7月の呼びかけ」2014.7.1. 情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/txt/2014/07outline.html>

(47)「2014年1月の呼びかけ」2014.1.7. 情報処理推進機構ウェブサイト <http://www.ipa.go.jp/security/txt/2014/01outline.html>

(48) 非合法な活動が行われるサイト。アングラサイトとも呼ばれる。非合法な薬物、武器や銀行口座、携帯電話の名義、個人情報、マルウェア、不正プログラム等が売買されていたり、サイトを通じて犯罪行為の仲間を募るなどの目的で利用されていたりする。国内でも実際に闇サイトを通じて、殺人事件や誘拐事件が起きた事例もあり、問題視されている。「（時時刻刻）闇サイト、犯罪誘う　偽名、求人も実行も」『朝日新聞』2007.9.6.

存在しており、マルウェアや攻撃ツール等が売買されていたり、ハッキングやDDoS（Distributed Denial of Service）攻撃の請負等の取引がされている。例えばDDoS攻撃であれば、1日の攻撃で30～70米ドルで取引されている(49)。また、闇サイトでは「Tor」（「トーア」と読む。）(50)等の匿名化ソフトを利用することで身元が追跡できない方法でアクセスすることが可能であるため、利用者の特定が難しい。また、海外サイトを中心にインターネット上の新たな取引手段として普及している仮想通貨ビットコインが違法取引に使われる事例も多く、その匿名性が取引の追跡を困難にしている。

近年、欧米では闇サイトに対する摘発が強化されており、2013年10月、Torで運営されていた巨大麻薬取引サイト「Silk Road」が米国連邦捜査局（FBI）によって摘発された。薬物以外にもマルウェアや違法コンテンツ、クレジットカード情報、ハッキングサービス等も取引されていたとされる(51)。また、2014年11月、欧州刑事警察機構（ユーロポール）は欧州16か国と米国の捜査当局と連携して、Torを利用して運営されていた闇サイトを摘発し、違法取引や闇市場の運営に係っていた17人を逮捕するとともに410以上のTorによる匿名化ドメインをダウンさせ、100万米ドル相当のビットコインや18万ユーロの現金、不正薬物、金銀などを押収している(52)。

## Ⅳ　インターネットの政治への影響力の拡大

### 1　民主化運動におけるインターネットの役割

諸外国に続き、国内でも2013年にインターネット等を利用した選挙運動が解禁されるなど、政治活動のツールとしてもインターネットが広く利用されるようになっている(53)。一方、海外では政府機関によるインターネットの検閲や監視により、インターネット上における政治的な活動が制限されている国も多くある。

こうした中、2010年頃からインターネットやSNSが強力な武器となり、国の政治を動かす事態が世界各地で起きている。

2010年から2011年にかけて中東・北アフリカで発生した民主化運動（いわゆる「アラブの春」）においては、市民同士の連絡や国内外への情報発信においてTwitterやFacebook等のSNSが大きな役割を果たした。表3にアラブの春をめぐる主な事件と市民のSNSの利用状況を示す。

---

(49) Pierluigi Paganini,“Cybercrime and the Underground Market,”2013.1.15. InfoSec Institute Website <http://resources.infosecinstitute.com/cybercrime-and-the-underground-market/>

(50) TCP/IPの通信経路の匿名化を行うソフトウェア。2012年に発生したPC遠隔操作事件（総論「情報通信技術の進展とサイバーセキュリティ」表3参照）においても、犯人が接続元を隠ぺいするために用いたとされている。

(51)「FBI、不正薬物の闇市場「Silk Road」を摘発」『ITmediaエンタープライズ』2013.10.3. <http://www.itmedia.co.jp/enterprise/articles/1310/03/news031.html>

(52)「Tor使った闇サイト、欧州と米国で一斉摘発」『ITmediaニュース』2014.11.10. <http://www.itmedia.co.jp/news/articles/1411/10/news045.html>

(53) 三輪和宏「諸外国のインターネット選挙運動」『調査と情報―ISSUE BRIEF―』518号, 2006.3.6, p.10. <http://dl.ndl.go.jp/view/download/digidepo_1000670_po_0518.pdf?contentNo=1>;「インターネット選挙運動解禁（公職選挙法の一部を改正する法律）の概要」pp.4-15. 総務省ウェブサイト <http://www.soumu.go.jp/main_content/000224709.pdf>

表3 「アラブの春」をめぐる主な事件

| 国･期間 | 概要 |
|---|---|
| チュニジア<br>2010年12月<br>〜<br>2011年3月 | ・2010年12月にチュニジア南部の町Sidi Bousid（シディ・ブジッド）で起きた、失業中の26歳の青年が、無許可で路上販売を行っていたことに対して、警察官から度重なる嫌がらせを受け、焼身自殺を図った事件をきっかけに、職を得る権利、発言の自由化、大統領周辺の腐敗の処罰などを求め、全国各地で連日ストライキやデモを行った。こうしたデモは長期政権そのものに対するデモへと急速に展開し、2011年1月に23年に及ぶベン・アリ政権が崩壊した（ジャスミン革命と呼ばれる）。<br>・抗議デモが広がるにつれ、その様子を撮影した画像や動画が、Facebook、YouTubeに次々とアップロードされた。Facebook上に作成された政府に抗議する複数のグループには、1週間で1万人以上が新たに参加し、YouTubeでは動画が3万件にも及んだ。また、Twitterでは関連のコメントが大量に投稿され、情報が拡散した。 |
| エジプト<br>2011年1月<br>〜<br>2011年2月 | ・ジャスミン革命をきっかけに2011年1月から大規模な反政府デモが発生し、約1か月後の2月にムバラク政権はエジプト軍最高評議会に国家権力を譲渡した（エジプト革命と呼ばれる）。<br>・Facebook、YouTube、Twitpic等のサイトを通じてインターネット上で画像・動画等多くの情報が拡散した。反政府に係る情報共有のために2010年頃から急速に登録者が拡大したFacebookページ“We are all Khaled Said”を中心にデモ参加者間の情報共有などが活発化した。同サイトは大規模デモ（2011年1月25日）の計画を宣言し、9万人以上の参加者が登録したとされる。<br>・エジプト政府はこうした反政府デモの混乱を鎮圧するために、Twitterの接続をブロックした後、広い地域において1月28日から5日間にわたりインターネット接続を遮断した。 |
| リビア<br>2011年2月<br>〜<br>2011年8月 | ・2011年2月15日に発生した人権活動家の弁護士の釈放要求デモをきっかけにカダフィ大佐の退陣を求めるデモが国内で拡大し、2011年8月にカダフィ政権が崩壊するに至った。<br>・インターネットインフラを厳重に制御していた旧政府は、デモの拡大を受け2月18日には同国内のインターネットの接続を遮断し、とりわけFacebookやTwitter等のSNS、アルジャジーラの報道サイトの遮断から始めたとされる。 |
| イエメン<br>2011年1月<br>〜<br>2012年2月 | ・2011年2月サーレハ大統領（当時）の退陣を求める反政府抗議活動が発生。2011年11月、同大統領は副大統領に大統領権限を移譲することに同意し、12月に暫定政権が発足。<br>・教育水準やネット普及率は低いが、若年層の比率が高いことから、一部でソーシャルメディアが活用されている。いわゆる活動家が始めたソーシャルメディア上のキャンペーン等が展開し、多くのイエメン人が、TwitterやFacebookでキャンペーンに参加し、宣伝に加わったとされる。中にはノーベル平和賞受賞者であるイエメンの反政府活動家も含まれ、Facebook上で同活動家のプロフィール写真をキャンペーンロゴとして使っている。 |

（出典）総務省情報通信国際戦略局情報通信経済室「情報通信産業・サービスの動向・国際比較に関する調査研究報告書（委託先：三菱総合研究所）」2012.3, pp.119-120. <http://www.soumu.go.jp/johotsusintokei/linkdata/h24_05_houkoku.pdf>等を基に三菱総合研究所作成。

また、香港では2014年9月から、2017年に予定されている香港行政長官選挙に関して、全国人民代表大会が民主派の候補を実質的に締め出す制度を決めたことに対して、学生を中心とする市民が抗議したデモが発生した。デモ参加者間の情報の拡散などに様々なSNSが利用された。香港では厳しいインターネットの検閲が行われている中国本土とは異なり、無検閲のインターネットにアクセスすることができる。香港で最も普及しているメッセージアプリのWhatsApp（ワッツアップ）のほか、警官隊の制圧に対抗するため、メッセージの暗号化サービスを提供するTelegram（テレグラム）、インターネットや電話回線につながっていなくてもユーザ同士のコミュニケーションが可能なFireChat（ファイアーチャット）なども広がったという(54)。

一方、中国政府は、香港の抗議行動が中国本土へ波及することを警戒して報道規制を強めており、日本の日本放送協会（NHK）や英国放送協会（British Broadcasting Corporation: BBC）の国際

(54)「香港民主化デモで活躍するSNS―連絡に混乱も」『ウォール・ストリート・ジャーナル日本版』2014.10.10. <http://jp.wsj.com/articles/SB11713596470002413933104580205880427493198>

放送では、デモに関するニュースの映像や音声が遮断されている。インターネット上でも、中国本土でTwitterに似たサービスを提供する中国の「微博（ウェイボ）」上で香港のデモを指す「雨傘革命」が検索できないほか、中国の検索サービスの「百度（バイドゥ）」では、香港の中心部占拠を意味する「占中」を検索すると、中国メディアの香港デモに対する批判的な報道が表示される状態となっている。また、通常は中国本土でもアクセス可能なFacebook傘下の写真共有サイトInstagram（インスタグラム）へのアクセスも遮断された。(55)

## 2　インターネットを使った内部告発

政府機関や企業に関する内部告発の手段としてインターネットが利用される事例が増えている。投稿者が匿名で政府、企業等に関する機密文書を公開するウェブサイトWikiLeaksは2010年11月から米国国務省の外交公電(56)約25万件を公開した。公開された外交公電には各国の外交機密に関する内容も含まれており、当時の米国大統領報道官は声明で、機密の公電公表を「無謀で危険な行為」と厳しく非難し、公電に含まれている外国政府との秘密の外交交渉が新聞で公表されれば「米国だけでなく、同盟諸国や友好国の外交利益にも大きな影響が及ぶ可能性がある」(57)と懸念を表明した。一方、WikiLeaksから事前に公電の提供を受けた米ニューヨークタイムズ紙は「国家安全保障を損なう公電を排除するなど配慮した」と説明した上で「国民の知る権利」や「真実の追究」を掲げて公表の正当性を主張した(58)。公開された外交公電の中には東京発の公電も5,697点含まれていた。いずれも2006年以降の文書で、1,660点は「機密文書」に該当するものだった(59)。

これと同時期、日本でも、国家公務員による機密情報の意図的な流出が発生した。2010年9月、尖閣諸島周辺の日本領海において、海上保安庁の巡視船が中国漁船に領海外に退去するよう警告を行っている最中に漁船側から衝突され、中国人船長を公務執行妨害等容疑で逮捕する事件が起こった。この事件に関して、同年11月に第五管区海上保安本部の職員（当時）が、事件の際の衝突映像をインターネット上に流出させるという事案が発生した(60)。海上保安庁では2010年12月に情報流出再発防止対策検討委員会が設置され、再発防止策が検討された。事件に直接関係のない職員が映像を入手し持ち出せる状況にあったこと、組織の方針に反して職員が故意に情報を流出させたという状況もあり、国の機密情報の管理の在り方について様々な問題を提起することとなった。

(55)「香港民主派、学生、デモ反対派と衝突　中国、強硬対応なお慎重、「天安門」再現を政府懸念」『日本経済新聞』2014.10.4;「香港デモ10万人参加　中国当局、「違法」と非難、TV報道遮断」『日本経済新聞』2014.10.2.

(56) 外務当局と海外の在外公館、又は在外公館間で電信によりやり取りされる公式文書。在外公館と駐在国の高官や政府関係者との間の会談の内容等も含まれる。

(57)「特集・ウィキリークス 露大統領は脇役の「ロビン」」『時事ドットコム』2010.12.6. <http://www.jiji.com/jc/v2?id=20101206wikileaks_09>

(58) 同上

(59)「内部告発サイト、米「国益損なう行為」東京発公電5697点」『日本経済新聞』2010.11.29, 夕刊.

(60) 海上保安庁編『海上保安レポート2011』2011, p.5.

### 3　過激主義組織によるインターネットを使ったプロパガンダ

「イスラム国」と呼ばれるイスラム教スンニ派過激組織は世界中から戦闘員を集めるため、SNSを効果的に使って組織の理念を発信したり、潜在的な戦闘員候補に接触し勧誘するなどのプロパガンダを行っている(61)。また、残忍な処刑の様子をインターネット上に公開するなど、人々に恐怖心を植え付けるとともに組織の強さや信仰心の厚さをアピールしている。全世界で現状の社会や生活に不満を抱える若い世代の一部が、こうした活動に魅了されて、「イスラム国」の戦闘員に参加しており(62)、各国が警戒を強めている。TwitterやYouTube等のサービスは「イスラム国」のアカウントや関連する画像を削除する等の対応を行っているが、「イスラム国」が次々に別のアカウントを作成したり、オープンソースの分散型SNS（SNS提供者のサーバだけでなく、ユーザが自由にサーバを立ててデータの保存が可能。）の利用を始めるなどいたちごっこが続いている(63)。

執筆：株式会社三菱総合研究所　情報通信政策研究本部　研究員　丸田（まるた）　佳織（かおり）
監修：神戸大学大学院工学研究科　教授　森井（もりい）　昌克（まさかつ）
京都産業大学法務研究科　客員教授
慶應義塾大学　名誉教授・弁護士　安冨（やすとみ）　潔（きよし）

(61)「SNS活用し戦闘員集めるイスラム国―当局の追跡も容易」『ウォール・ストリート・ジャーナル日本版』2014.8.29. <http://jp.wsj.com/articles/SB10001424052970203483604580120522168233204>
(62)「特集ワイド：今さらですが「イスラム国」とは？ SNSで戦闘員、続々」『毎日新聞』2014.10.9, 夕刊.
(63)「イスラム過激派、勧誘や脅迫にソーシャルメディア駆使」『AFPBB News』2014.8.21. <http://www.afpbb.com/articles/-/3023673>;「Twitterから閉めだされた「イスラム国」、分散型SNSのDiasporaに乗り換え」『ITmediaニュース』2014.8.22. <http://www.itmedia.co.jp/news/articles/1408/22/news099.html>